

Afbeelding van de Advanced Malware Protection Private Cloud PC3000 en zet de back-up terug

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u het apparaat voor Advanced Malware Protection (AMP), Private Cloud-hardware, opnieuw naar de fabriekstoestand kunt terugbrengen en vervolgens de back-up kunt herstellen. Als u het apparaat gewoon wilt terugzetten naar de fabriekstoestand, overslaat u stap 8 en volgt u de gebruikelijke installatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Advanced Malware Protection Private Cloud PC3000
- Kernel-gebaseerde Virtual Machine (KVM)-toegang via Cisco Integrated Management Controller (CIMC)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Advanced Malware Protection Private Cloud PC3000 3.1.1
- Chrome browser om toegang te krijgen tot de KVM-console

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Stap 1. Meld u aan bij CIMC. Open de KVM-console.

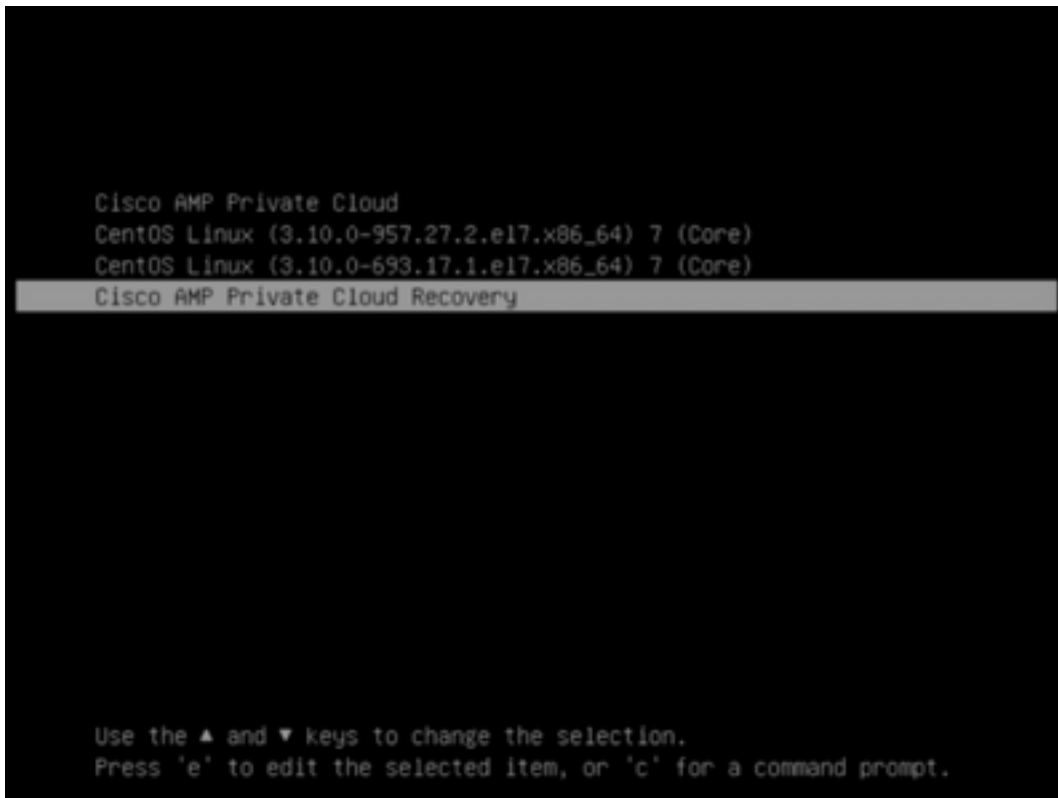
Zorg ervoor dat pop-ups zijn ingeschakeld voor die pagina in de browser.

Stap 2. Neem het apparaat opnieuw in.

U kunt het apparaat opnieuw opstarten via het beheerportal, Secure Shell (SSH) of CIMC KVM.

Stap 3. Nadat het Basic Input Output System (GNU) Power-on-zelftest (POST) is voltooid, wordt het menu GNU GR en Unified Bootloader (GRUB) weergegeven:

Selecteer **Cisco Advanced Malware Protection Private Cloud Restore > Opties voor opnieuw installeren > Applicatie opnieuw installeren**.



Attempt Regular Boot
Recovery Boot
Appliance Reinstall Options
Wipe Appliance Options
Boot previous Recovery Boot version



Press enter to boot the selected OS, "e" to edit the commands before booting or "c" for a command-line.

Appliance Reinstall
Attempt Regular Boot
Recovery Menu

The appliance will be re-installed to factory defaults. Using this functionality requires the following credentials to be entered.

Username: reinstall
Password: yes

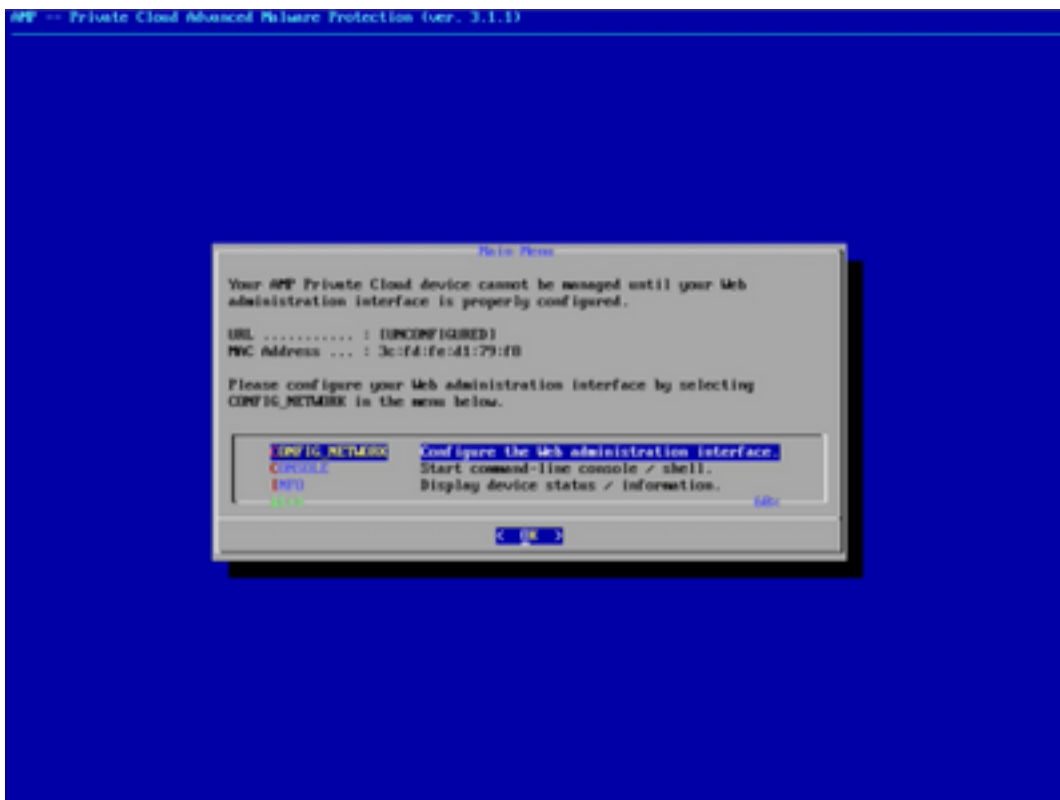


Press enter to boot the selected OS, "e" to edit the commands before booting or "c" for a command-line.

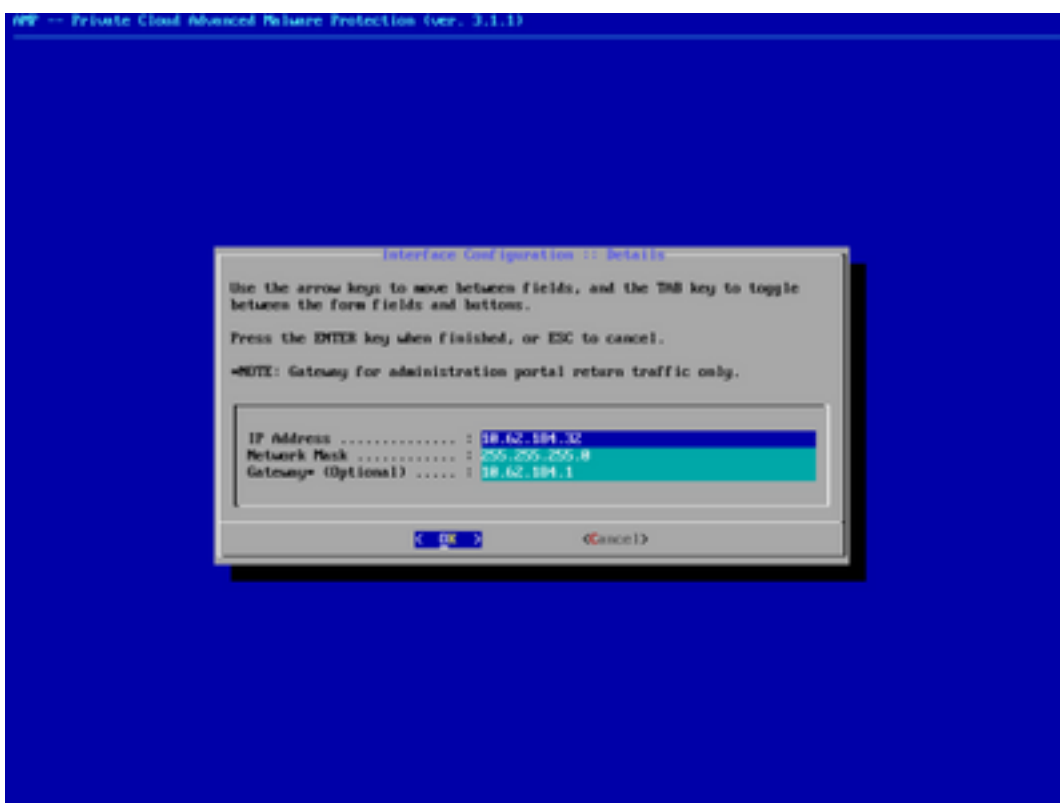
Stap 4. Voer een gebruikersnaam en een wachtwoord in.

Username: herinstalleren

Wachtwoord: ja



Stap 6. Het netwerk configureren in het submenu CONFIG_NETWORK.



Stap 7. Meld u aan bij het AMP OPadmin-portal met het wachtwoord uit stap 5.



Password Required

Authentication is required to administer your AMP for Endpoints Private Cloud device. The password can be found on the device console of your Private Cloud device.

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

[Password Recovery](#)

Support

Step 8. Gebruik SFTP of SCP om back-up te downloaden van externe server naar /gegevens/.



Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode ✓
- Standalone Operation ✓
- AMP for Endpoints Console Account ✓
- Hardware Configuration

Configuration

- Network ✓
- Date and Time ✓
- Certificate Authorities ✓
- Upstream Proxy Server ✓
- Email ✓
- Notifications ✓
- Backup ✓
- SSH ✓
- Syslog ✓
- Updates ✓

Services

- Authentication ✓
- AMP for Endpoints Console ✓
- Disposition Server ✓
- Disposition Server ✓
- Extended Protocol ✓
- Disposition Update ✓
- Service ✓
- Preprocessor Management Center ✓

Other

- Review and Install

Start Installation

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Preparing Restore

Your restore file is being processed, please wait.

- + Adding mongo_event_consumer account.
 - + Running startup script to generate new password. Generating a random password for mongo_event_consumer
 - + Removing the .rpmnew file
 - + Removing event_mongo_store service
 - + Adding firehose_cassandra account.
 - + Running startup script to generate new password. Generating a random password for firehose_cassandra
- Checking for bios and lmc updates. This may take some time. If an update is available and the update is successful, you will be asked to reboot the box.

Clean Installation

Start

Restore

Local Remote **Upload**

Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

+ Choose Restore File

Start

Restore

Local Remote Upload

Restore from a backup file present on the device. Files will be extracted to the directory your backup is located in during the restore process; for this reason, it is recommended that the file be located in the /data directory.

/data/amp.bak

Stap 9. Controleer de hardwareconfiguratie, klik op **Volgende > Installatie starten**.

CISCO AMP for Endpoints Private Cloud Administration Portal Help Logout

Configuration Operations Status Integrations Support Standalone

Hardware Configuration

	Installed	Minimum Required
CPU Cores	48	8
Memory	1510 GB	128 GB

Next >

Start Installation

- Installation Options
 - Install or Restore ✓
 - License ✓
 - Welcome ✓
 - Deployment Mode ✓
 - Standalone Operation ✓
 - AMP for Endpoints Console ✓
 - Account ✓
 - Hardware Configuration
- Configuration
 - Network ✓
 - Date and Time ✓
 - Certificate Authorities ✓
 - Upstream Proxy Server ✓
 - Email ✓
 - Notifications ✓
 - Backup ✓
 - SSH ✓
 - Synlog ✓
 - Updates ✓
- Services
 - Authentication ✓
 - AMP for Endpoints Console ✓
 - Disposition Server ✓
 - Disposition Server ✓
 - Extended Protocol ✓
 - Disposition Update ✓
 - Service ✓
 - Firepower Management Center ✓
- Other
 - Review and Install

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > Standalone Operation ✓
- > AMP for Endpoints Console Account ✓
- > Hardware Configuration ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > AMP for Endpoints Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firewall Management Center ✓

Other

- > Review and Install

Start Installation

Review and Install

Review the following information and, once you are satisfied with your configuration settings, begin the installation. Note that the configuration shown below cannot be altered after installation.

Restore Ready

Your configuration has been restored, and your data will be restored during installation. You may review and edit some parts of your configuration before proceeding with installation.

Installation Type ✎ Edit

Standalone Connected

- Requires an Internet Connection
- Communication with AMP for Endpoints Connectors managed by this device are needed.
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates may be downloaded separately or automatically on this device.

AMP for Endpoints Console Account ✎ Edit

Name	Wojciech Cecot
Email Address	wcecot@cisco.com
Business Name	Cisco - wcecot

Recovery

When restoring from a backup, a recovery image is not required.

Start Installation

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
▶ Pending	Tue May 12 2020 10:05:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 0 minute, 46 seconds ago	⊙ Please wait...	⊙ Please wait...

Your device will need to be rebooted after this operation.

Reboot

Output

```

[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/ruby.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/network.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/powershell.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/os.rb
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -s' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -r' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -v' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -m' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -p' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -o' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'env lscod' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin LSB: ran 'lsb_release -a' and returned 0
    
```

Download Output

Stap 10. De computer moet opnieuw worden opgestart nadat het product met succes is hersteld.

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
✔ Successful	Tue May 12 2020 10:05:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 34 minutes, 19 seconds ago	Tue May 12 2020 10:22:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 17 minutes, 19 seconds ago	0 day, 0 hour, 16 minutes, 59 seconds

Your device will need to be rebooted after this operation.

[Reboot](#)

Output

```
[2020-05-12T00:22:15+00:00] INFO: Skipping cleanup of resource table files and links
[2020-05-12T00:22:15+00:00] INFO: Running report handlers
[2020-05-12T00:22:15+00:00] INFO: Report handlers complete
[2020-05-12T00:22:15+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2020-05-12T00:22:15+00:00] DEBUG: Audit Reports are disabled, skipping sending reports.
[2020-05-12T00:22:15+00:00] DEBUG: Forked instance successfully reaped (pid: 97568)
[2020-05-12T00:22:15+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.

=====
Chef run finished successfully
=====

Installation has finished successfully! Please reboot!
=====
```

[Download Output](#)

Verifiëren

Controleer na het opnieuw opstarten van het apparaat of beide portalen goed werken. Probeer OPadmin en console portal in de webbrowser te openen. Het kost een paar minuten om beide portalen toegankelijk te maken.

Problemen oplossen

In geval van back-up-herstelproces zijn het wachtwoord voor OPadmin en Console-poorten hetzelfde als voorheen. Anders moet u gebruiken wat u in de wizard hebt ingesteld.